Journal of Number Theory **76**, 1–15 (1999)
Article ID jnth.1998.2344, available online at http://www.idealibrary.com on IDEAL®

Approche algorithmique du groupe des classes logarithmiques

F. Diaz y Diaz

Laboratoire A2X, Université de Bordeaux I, 351, Cours de la Libération, 33405 Talence Cedex, France
E-mail: diaz@math.u-bordeaux.fr

et

F. Soriano

Communicated by M. Pohst

Received October 8, 1996; revised July 1, 1998

In this paper we study, from an algorithmic point of view, the structure of the l-part of the logarithmic class group for abelian number fields whose interest is related to K-theory. All the computations on this group are performed using the PARI package. © 1999 Academic Press

1. INTRODUCTION

Dans ce travail, le nombre entier l est fixé une fois pour toutes. Pour un corps de nombres K, nous considérons les deux pro-l-extensions suivantes de K qui sont en liaison avec la K_2-théorie: la l-extension localement cyclotomique de K notée K^{lc} et la l-extension cyclotomique de K notée K^c. La difficulté de l'étude du groupe de Galois de K^{lc}/K^c incite à l'introduction d'un l-groupe de classes pouvant être construit explicitement par des méthodes numériques. Défini par Jaulent (cf. [J$_3$]), ce groupe est appelé le l-groupe des classes logarithmiques de K et est noté $\widetilde{\mathcal{C}l}_K$ (ou plus simplement $\widetilde{\mathcal{C}l}$ lorsque aucune confusion n'est à craindre quant au choix du corps de nombres considéré). On a ainsi un isomorphisme

$$\widetilde{\mathcal{C}l} \simeq \mathrm{Gal}(K^{lc}/K^c).$$

0022-314X/99 $30.00

L'intérêt apporté aux classes logarithmiques concerne le lien entre ce groupe et le noyau hilbertien (ou sauvage) de K. En effet, lorsque le corps K contient les racines primitives $2l$-ièmes de l'unité et si l'on désigne par μ_l le sous-groupe de torsion d'ordre l de $K^\times$, il existe un isomorphisme canonique (cf. [J_2]).

$$\mu_l \otimes_{\mathbb{Z}} \widetilde{\mathscr{C}l} \simeq H_2/H_2^l$$

entre le quotient d'exposant l du l-groupe des classes logarithmiques du corps K et le sous-groupe des éléments d'ordre au plus l de son noyau hilbertien dans le groupe universel K_2 pour les symboles sur K. Nous présentons ici un algorithme permettant de déterminer la structure du l-groupe des classes logarithmiques et qui peut être appliqué (en principe) à tout corps de nombres contenant les racines $2l$-ièmes de l'unité. Il nous a permis d'obtenir de nouveaux exemples de corps quartiques dont l-rang de la l-partie du noyau hilbertien est non triviale pour $l=2$ et $l=3$. Par exemple, nos calculs montrent que le 3-groupe des classes logarithmiques de $\mathbb{Q}(\sqrt{-3}, \sqrt{1901})$ a trois composantes cycliques si bien que le 3-rang du noyau hilbertien de ce corps est 3 (cf. Section 6).

Les techniques algorithmiques que nous avons utilisées pour construire le groupe des classes logarithmiques s'inspirent des méthodes dites sous-exponentielles de Hafner et McCurley [H-M] dont une description détaillée est donnée par Diaz y Diaz et Olivier [D-O]. Pour connaître un groupe abélien fini, et en particulier un groupe de classes, il suffit de déterminer un système de générateurs de ce groupe et de donner une matrice de relations liant ces générateurs de sorte que toute autre relation puisse s'exprimer comme combinaison linéaire à coefficients entiers rationnels (pouvant éventuellement être des approximations d'entiers l-adiques) des colonnes de la matrice. Il est souvent utile d'appliquer à une telle matrice une réduction à sa forme normale d'Hermite (HNF) (ce qui ne modifie en rien les générateurs choisis) et de poursuivre par une réduction de Smith (SNF). Ce procédé standard permet de déterminer explicitement une matrice diagonale dont les termes diagonaux sont $[d_1, d_2, ..., d_n]$ avec $d_i \mid d_{i-1}$, $d_n > 1$ et un système de générateurs $[g_1, g_2, ..., g_n]$ de sorte que le groupe considéré puisse s'écrire, dans ces conditions, sous la forme

$$(\mathbb{Z}/d_1\mathbb{Z})\, g_1 \oplus \cdots \oplus (\mathbb{Z}/d_n\mathbb{Z})\, g_n.$$

D'autre part, on fait un large usage de la solution du logarithme discret dans le cadre qui suit (cf. [C]): lorsque g est un élément d'un groupe abélien fini, connu dans le sens précédemment précisé, il est possible de déterminer le vecteur d'exposants $[a_1, a_2, ..., a_n]$ tel qu'on ait

$$g = g_1^{a_1} g_2^{a_2} \cdots g_n^{a_n}.$$

Comme le calcul du groupe des classes logarithmiques est basé sur la connaissance du groupe des classes $\mathscr{C}l$ au sens ordinaire, on doit tenir compte du fait que les méthodes sous-exponentielles donnent un résultat dépendant de la validité de l'hypothèse de Riemann généralisée pour la fonction Zeta de Dedekind du corps K. En fait, il est possible (et les algorithmes existent, par exemple, dans PARI [P]) de "certifier" la validité des résultats obtenus en appliquant le logarithme discret à tous les idéaux dont la norme est plus petite que la borne de Zimmert (cf. [D-O]), mais ceci n'a pas été fait en ce qui concerne les résultats numériques donnés dans la Section 6.

Tous les algorithmes décrits dans ce travail ont été programmés en utilisant le système PARI.

Précisons enfin quelques notations. Pour un corps de nombres K, si $\mathfrak{a}$ appartient au tensorisé l-adique du groupe des idéaux entiers de K, nous notons $[\mathfrak{a}]$ sa classe dans $\widetilde{\mathscr{C}l}$ (lorsque $\mathfrak{a}$ est de degré nul) et $\{\mathfrak{a}\}$ sa classe dans le tensorisé l-adique du groupe des classes d'idéaux (ou éventuellement, lorsque aucune confusion n'est à craindre, sa classe dans le $\mathbb{Z}_l$-tensorisé du groupe des l-classes). D'autre part, nous avons gardé la notation additive pour les diviseurs représentant les classes logarithmiques et la notation multiplicative pour la structure du groupe des idéaux fractionnaires non nuls de K. L'utilisation, dans ce dernier cas, de la notation matricielle est faite comme dans [C] et ne présente aucune ambiguïté.

2. RAPPELS ET DEFINITIONS (CF. [J_3])

Soit K un corps de nombres fixé. On note P l'ensemble des places finies de K et $\mathscr{D}$ le $\mathbb{Z}_l$-module libre $\bigoplus_{\mathfrak{p} \in P} \mathbb{Z}_l \mathfrak{p}$ qu'on identifie canoniquement au tensorisé $\mathbb{Z}_l \otimes_{\mathbb{Z}} D \simeq \bigoplus_{\mathfrak{p} \in P} \mathfrak{p}^{\mathbb{Z}_l}$ du groupe $D = \bigoplus_{\mathfrak{p} \in P} \mathfrak{p}^{\mathbb{Z}}$ des diviseurs au sens ordinaire de K. Le module $\mathscr{D}$ est appelé le l-groupe des diviseurs logarithmiques de K.

A chaque place $\mathfrak{p} \in P$ au-dessus de p on associe un premier invariant noté $\tilde{e}_{\mathfrak{p}}$ et appelé l'indice de ramification logarithmique de $\mathfrak{p}$. Il est défini comme l'entier dont:

(i) les q-parties coïncident avec celles des indices de ramification usuels $e_{\mathfrak{p}}$ pour chaque premier $q \neq p$,

(ii) la p-partie est donnée par l'indice $(h_p(\mathscr{K}_{\mathfrak{p}}^{\times}) : \mathbb{Z}_p)$ où h_p est l'application

$$h_p(\cdot) = -\frac{\operatorname{Log} |\cdot|_{\mathfrak{p}}}{p \cdot [K_{\mathfrak{p}} : \mathbb{Q}_p]} \qquad \text{si} \quad p \neq 2,$$

$$h_p(\cdot) = -\frac{\operatorname{Log} |\cdot|_{\mathfrak{p}}}{4 \cdot [K_{\mathfrak{p}} : \mathbb{Q}_p]} \qquad \text{si} \quad p = 2,$$

définie comme l'opposé du quotient du logarithme d'Iwasawa de la valeur absolue p-adique principale par le produit du degré fini $[K_{\mathfrak{p}} : \mathbb{Q}_p]$ et du degré p-adique du nombre premier p.

On introduit ensuite un second invariant noté $\tilde{f}_{\mathfrak{p}}$ et appelé le degré résiduel logarithmique. Il est défini comme l'entier pour lequel on a la relation $\tilde{e}_{\mathfrak{p}} \tilde{f}_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$ où $e_{\mathfrak{p}}, f_{\mathfrak{p}}$ sont, respectivement, l'indice de ramification et le degré résiduel usuels de l'idéal $\mathfrak{p}$ dans l'extension $K/\mathbb{Q}$.

On définit ensuite sur P l'application degré, à valeurs dans $\mathbb{Z}_l$, par la formule

$$\deg_K \mathfrak{p} = \tilde{f}_{\mathfrak{p}} \deg p$$

où $\deg p$ est le degré l-adique du nombre premier $p \in \mathfrak{p}$ dont la valeur est

(i) $\deg p = \log p$ si $(p \neq l)$,

(ii) $\deg l = l$ si $(l \neq 2)$,

(iii) $\deg 2 = 4$,

$\log p$ désignant le logarithmique l-adique de p. On étend l'application $\deg_K$ à $\mathscr{D}$ tout entier par $\mathbb{Z}_l$-linéarité et l'on obtient la suite exacte de $\mathbb{Z}_l$-modules

$$0 \to \tilde{\mathscr{D}} \to \mathscr{D} \to \deg_K \mathscr{D} \to 0$$

où $\tilde{\mathscr{D}}$ est le sous-module de $\mathscr{D}$ des diviseurs logarithmiques de degré nul.

J.-F. Jaulent (cf. [J$_3$]) a associé à chaque place $\mathfrak{p} \in P$ une valuation $\tilde{v}_{\mathfrak{p}}$, dite valuation logarithmique, définie sur $\mathscr{K} = \mathbb{Z}_l \otimes_{\mathbb{Z}} K^{\times}$ et qu'il a reliée au symbole hilbertien attaché à $\mathfrak{p}$. Cette valuation est donnée par

$$\tilde{v}_{\mathfrak{p}}(\cdot) = -\frac{f_{\mathfrak{p}}}{\tilde{f}_{\mathfrak{p}}} v_{\mathfrak{p}}(\cdot) \qquad \text{si} \quad \mathfrak{p} \nmid l$$

$$\tilde{v}_{\mathfrak{p}}(\cdot) = -\frac{\mathrm{Log}\, |\cdot|_{\mathfrak{p}}}{\deg_K \mathfrak{p}} \qquad \text{si} \quad \mathfrak{p} \mid l,$$

où $v_{\mathfrak{p}}$ désigne la $\mathfrak{p}$-valuation usuelle et $\mathrm{Log}\, |\ |_{\mathfrak{p}}$ le logarithme d'Iwasawa de la valeur absolue l-adique principale.

Lorsque la place $\mathfrak{p}$ ne contient pas l, les valuations logarithmique et usuelle sont liées par la formule $v_{\mathfrak{p}} = \lambda_{\mathfrak{p}} \tilde{v}_{\mathfrak{p}}$ où $\lambda_{\mathfrak{p}} = \tilde{e}_{\mathfrak{p}}/e_{\mathfrak{p}} = f_{\mathfrak{p}}/\tilde{f}_{\mathfrak{p}}$ est inversible dans $\mathbb{Z}_l$. À l'aide de cette valuation, on obtient un homomorphisme canonique de $\mathbb{Z}_l$-modules, noté $\tilde{d}$, qui associe à chaque $x \in \mathscr{K}$ le diviseur logarithmique

$$\tilde{d}(x) = \sum_{\mathfrak{p} \in P} \tilde{v}_{\mathfrak{p}}(x)\, \mathfrak{p}$$

dont l'image, $\widetilde{\mathscr{P}} = \tilde{d}(\mathscr{K})$, est le l-groupe des diviseurs logarithmiques principaux de K.

D'après la formule du produit $\widetilde{\mathscr{P}}$ est un sous-module de $\widetilde{\mathscr{D}}$ et le quotient $\widetilde{\mathscr{C}l} = \widetilde{\mathscr{D}}/\widetilde{\mathscr{P}}$ est appelé le l-groupe des classes logarithmiques de K. La conjecture de Gross, démontrée dans le cas abélien et dans certains cas de corps totalement réels (cf. [J_4]), affirme que $\widetilde{\mathscr{C}l}$ est un groupe abélien fini (cf. [J_1]).

Désormais K est supposé galoisienne; cette hypothèse entraîne en particulier l'égalité des degrés de deux places conjuguées.

3. CARACTERISATION DU l-GROUPE DES CLASSES LOGARITHMIQUES

Soit $\mathscr{C}l$ le tensorisé l-adique du groupe de classes de K au sens ordinaire. On note $\mathscr{C}l'$ le quotient de $\mathscr{C}l$ par le sous-groupe engendré par les classes représentées par les idéaux de K au-dessus de l. (Autrement dit, $\mathscr{C}l'$ désigne le l-groupe des l-classes).

LEMME 1. *L'application* φ: $\widetilde{\mathscr{C}l} \to \mathscr{C}l'$ *qui associe à chaque classe d'un diviseur logarithmique de degré nul* $\sum_{\mathfrak{p} \in P} m_{\mathfrak{p}} \mathfrak{p}$ *la classe représentée par l'idéal* $\prod_{\mathfrak{p} \nmid l} \mathfrak{p}^{\lambda_{\mathfrak{p}} m_{\mathfrak{p}}}$, *est un homomorphisme de groupes. De plus,* Ker $\varphi = \widetilde{\mathscr{C}l}(l)$ *où* $\widetilde{\mathscr{C}l}(l)$ *est le l-groupe des classes logarithmiques des diviseurs construits sur les places de K au-dessus de l.*

Démonstration. Soit $\tilde{\mathfrak{a}} = \sum_{\mathfrak{p} \in P} m_{\mathfrak{p}} \mathfrak{p}$ un diviseur logarithmique principal: il est donc de la forme $\tilde{\mathfrak{a}} = \tilde{d}(\alpha)$ pour un $\alpha \in \mathscr{K}$. Un représentant de l'image par φ de la classe de $\tilde{\mathfrak{a}}$ s'écrit alors, en termes d'idéaux, sous la forme: $\mathfrak{a} = \prod_{\mathfrak{p} \nmid l} \mathfrak{p}^{\lambda_{\mathfrak{p}} \tilde{v}_{\mathfrak{p}}(\alpha)} = \prod_{\mathfrak{p} \nmid l} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)} = (\alpha \mathbb{Z}_K) \times \prod_{i=1}^{g} \mathfrak{l}_i^{-v_{\mathfrak{l}_i}(\alpha)}$ où $\mathfrak{l}_i$ parcourt les g places de K au-dessus de l. Ceci montre que le morphisme φ est bien défini sur $\widetilde{\mathscr{C}l}$. La dernière affirmation du lemme est alors immédiate.

LEMME 2. *On a* Coker $\varphi \simeq \deg_K \mathscr{D}/(\deg_K \mathfrak{l})\, \mathbb{Z}_l$, *où* $\mathfrak{l}$ *est l'une quelconque des places sauvages* (*i.e. au-dessus de* l) *de K.*

Démonstration. D'après sa définition, l'image de φ est le sous-groupe des classes de $\mathscr{C}l'$ représentées par un idéal de la forme $\prod_{\mathfrak{p} \nmid l} \mathfrak{p}^{\lambda_{\mathfrak{p}} m_{\mathfrak{p}}}$ tel qu'il existe une famille $(m_{\mathfrak{l}_i})$ d'entiers l-adiques indexés sur les places au-dessus de l satisfaisant la relation: $\sum_{\mathfrak{p} \in P} m_{\mathfrak{p}} \deg_K \mathfrak{p} = 0$ ou encore $\sum_{\mathfrak{p} \nmid l} m_{\mathfrak{p}} \deg_K \mathfrak{p} = -(\sum_{i=1}^{g} m_{\mathfrak{l}_i}) \deg_K \mathfrak{l}$. Ceci montre que l'on a $\sum_{\mathfrak{p} \nmid l} m_{\mathfrak{p}} \deg_K \mathfrak{p} \in \mathbb{Z}_l \deg_K \mathfrak{l}$.

A présent, introduisons l'homomorphisme η de $\mathscr{C}l'$ dans le l-groupe $\deg_K \mathscr{D}/(\deg_K \mathfrak{l})\, \mathbb{Z}_l$, qui à toute classe représentée par l'idéal $\prod_{\mathfrak{p} \nmid l} \mathfrak{p}^{m_{\mathfrak{p}}}$, dont l'ordre est une puissance de l, associe la classe du degré du diviseur

$\sum_{\mathfrak{p} \nmid l} (m_{\mathfrak{p}}/\lambda_{\mathfrak{p}})\, \mathfrak{p}$ modulo le degré de $\mathfrak{l}$. Pour justifier son existence supposons que l'idéal $\prod_{\mathfrak{p} \nmid l} \mathfrak{p}^{m_{\mathfrak{p}}}$ puisse s'écrire sous la forme $\prod_{\mathfrak{p} \nmid l} \mathfrak{p}^{m_{\mathfrak{p}}} = (\alpha \mathbb{Z}_K) \cdot \prod_{i=1}^{g} \mathfrak{l}_i^{n_i}$. Un calcul élémentaire montre que l'on a

$$\sum_{\mathfrak{p} \nmid l} \frac{m_{\mathfrak{p}}}{\lambda_{\mathfrak{p}}}\, \mathfrak{p} = \widetilde{d}(\alpha) + \sum_{i=1}^{g} n_i' \mathfrak{l}_i \qquad \text{avec} \quad (n_i' \in \mathbb{Z}_l)$$

et que le degré du diviseur $\sum_{\mathfrak{p} \nmid l} (m_{\mathfrak{p}}/\lambda_{\mathfrak{p}})\, \mathfrak{p}$ est un multiple du degré de $\mathfrak{l}$. L'application $\deg_K$ étant un homomorphisme, nous savons désormais que η est bien défini et est un homomorphisme de l-groupes dont le noyau est exactement l'image de φ. Enfin, la suite exacte du paragraphe 2 caractérisant $\widetilde{\mathscr{D}}$ nous assure de la surjectivité de η. Le lemme est ainsi démontré.

D'après les deux lemmes précédents, on a la suite exacte

$$0 \to \widetilde{\mathscr{C}l}(l) \to \widetilde{\mathscr{C}l} \to \mathscr{C}l' \to \deg_K \mathscr{D}/(\deg_K \mathfrak{l})\, \mathbb{Z}_l \to 0$$

qui peut être écourtée en la suite exacte: $0 \to \widetilde{\mathscr{C}l}(l) \to \widetilde{\mathscr{C}l} \to H \to 0$ où H est le noyau de l'homomorphisme $[\mathscr{C}l' \xrightarrow{\eta} \deg_K \mathscr{D}/(\deg_K \mathfrak{l})\, \mathbb{Z}_l]$ introduit ci-dessus.

On a démontré le résultat suivant:

Théorème 3. *Un système de générateurs de l-groupe des classes logarithmiques de K est obtenu en joignant les générateurs du sous-groupe* $\widetilde{\mathscr{C}l}(l)$ *à un relèvement dans* $\widetilde{\mathscr{C}l}$ *d'un système de générateurs de H.*

Nous décrivons dans 5.1 un précédé de détermination des générateurs de $\widetilde{\mathscr{C}l}(l)$ et une matrice de relations liant ces derniers entre eux. De manière analogue, nous exposons dans le Lemme 5 de 5.3 le calcul d'un système de générateurs de H et la méthode d'obtention de la matrice de relations de ces générateurs. Finalement, on décrit dans 5.4 la manière de calculer la structure $\widetilde{\mathscr{C}l}$ et de déterminer des générateurs de ce groupe.

4. CALCULS EXPLICITES

4.1. *Calcul de la norme locale*

Soient $\alpha \in \mathbb{Z}_k$, $\alpha \neq 0$ et $\mathfrak{p}$ une place fixée de K au-dessus du nombre premier p. On suppose que l'idéal $\mathfrak{p}$ est connu par une représentation à deux éléments: $\mathfrak{p} = p\mathbb{Z}_K + \beta \mathbb{Z}_K$, avec $v_{\mathfrak{p}}(\beta) = 1$. Pour calculer la norme locale $N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\alpha)$ on procède de la manière suivante: le groupe de Galois $G = \{\sigma_1 = Id, ..., \sigma_n\}$ de l'extension $K/\mathbb{Q}$ peut être calculé explicitement par la donnée des conjugués $x_1 = x, ..., x_n = \sigma_n(x)$ d'un élément primitif x de l'extension $K/\mathbb{Q}$. Le groupe de décomposition D de $\mathfrak{p}$ est défini par

$D=\{\sigma\in G/v_{\mathfrak{p}}(\sigma(\beta)-\beta)\geqslant 1\}$ et, quitte à modifier l'élément primitif, on peut supposer que $\bar{x}=\sum_{\sigma\in D}\sigma(x)$ est un élément primitif de l'extension $K^D/\mathbb{Q}$ où K^D est le sous-corps de K fixé par D.

Dans K^D, l'idéal $p\mathbb{Z}_{K^D}$ se décompose comme produit de s idéaux premiers de degré résiduel 1 et un seul parmi eux, noté $\bar{\mathfrak{p}}$, est au-dessus de $\mathfrak{p}$. Le polynôme caractéristique de $\bar{x}\in K$ est la puissance d'un polynôme irréductible de degré s. A partir de ce polynôme, il est possible de déterminer une base d'entiers de K^D par des méthodes algorithmiques bien connues. On sait exprimer $\bar{x}$, en tant qu'élément de K, dans la base d'entiers de $\mathbb{Z}_K$. En faisant de même pour chacun des éléments de la base d'entiers de K^D, on obtient une matrice dont les colonnes sont, par construction, les coordonnées des entiers de la base de $\mathbb{Z}_{K^D}$ dans la base d'entiers de K. La détermination du noyau entier de la matrice obtenue par concaténation de la matrice dernièrement construite avec le vecteur colonne des coordonnées de $\bar{\alpha}=\prod_{\sigma\in D}\sigma(\alpha)$ dans la base d'entiers de K donne l'expression de $N_{K/K^D}(\alpha)$ dans la base d'entiers de K^D. Finalement, on peut factoriser le polynôme irréductible de $\bar{x}\in K^D$ dans le corps $\mathbb{Q}_p$. On obtient ainsi s racines dans $\mathbb{Z}_p$ dont une seule est associée à l'idéal $\mathfrak{p}$. On utilise cette racine pour identifier $K^D_{\mathfrak{p}}$ avec $\mathbb{Q}_p$, plonger $N_{K/K^D}(\alpha)$ dans $\mathbb{Q}_p$ et déterminer la valeur de la norme locale cherchée.

4.2. *Calcul de l'indice de ramification logarithmique*

Par construction, la p-partie de l'indice $\tilde{e}_{\mathfrak{p}}$ est p^{-m}, où m est la plus petite p-valuation des images par h_p des générateurs du p-complété profini $\mathcal{K}_{\mathfrak{p}}^{\times}=\lim_{\leftarrow} K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times p^n}$ du groupe multiplicatif $K_{\mathfrak{p}}^{\times}$. Si ζ est une racine primitive de l'unité d'ordre $N\mathfrak{p}-1$ dans $K_{\mathfrak{p}}^{\times}$ $(\mathfrak{p}\in P)$ lorsque p est impair ou bien $\zeta=\pm 1$ quand $N\mathfrak{p}=2$ et si l'on désigne par π une uniformisante locale en $\mathfrak{p}$, un système générateur de $K_{\mathfrak{p}}^{\times}$ est donné par la famille $\eta_{ij}\pi^k=(1+\zeta^i\pi^j)\,\pi^k$ où l'exposant j prend toutes les valeurs de 1 jusqu'à la partie entière de $pe_{\mathfrak{p}}/(p-1)+1$ (à l'exception des multiples de p), l'exposant i varie de 0 à $N\mathfrak{p}-2$ et k parcourt $\mathbb{Z}$. Cependant, la plus petite p-valuation de l'image $h_p(\eta_{ij}\pi^k)$ est atteinte pour $k=0$. En effet, comme la valeur absolue p-adique $|\pi|_{\mathfrak{p}}$ attachée à $\mathfrak{p}$ est une puissance de p $(p\in\mathfrak{p})$, nous avons les égalités successives

$$v_p(h_p(\eta_{ij}\pi^k))=v_p(h_p(\eta_{ij})+h_p(\pi^k))=v_p(h_p(\eta_{ij}))$$

qui montrent que le calcul de la p-valuation minimale est indépendante de k.

Finalement, nous retiendrons que la p-partie de l'indice de ramification logarithmique de $\mathfrak{p}$ dans l'extension $K/\mathbb{Q}$ est égale à $p^{-\min_{i,j}(v_p(h_p(\eta_{ij})))}$.

Du point de vue algorithmique, nous avons à déterminer une racine primitive $(N\mathfrak{p}-1)$-ième de l'unité. Commençons par considérer le plongement de K^D dans $\mathbb{Q}_p$ (cf. 4.1) permettant l'identification de $K^D_{\bar{\mathfrak{p}}}$ avec $\mathbb{Q}_p$ puis la matrice d'Hermite de l'idéal $\mathfrak{p}$. Il y a exactement f coefficients multiples de p dans la diagonale principale. Chacun d'eux détermine un élément w_{i_j} $(1 \leqslant j \leqslant f)$ de la base d'entiers de K de sorte qu'une combinaison linéaire de la forme $b=\sum_{j=i}^{f} a_j w_i$ où les entiers a_j vérifient $0 \leqslant a_j < p$, appartient à $\mathfrak{p}$ si et seulement si $a_j = 0$ pour $j = 1, ..., f$. On peut donc représenter chaque élément du corps résiduel $\bar{k}$ de $K_\mathfrak{p}$ par une telle combinaison linéaire et, en particulier, écrire chaque élément de $K_\mathfrak{p}$ sous la forme $b_0 + b_1\pi + b_2\pi^2 + \cdots$. Désormais $b_0 \neq 0$ est fixé. Il existe alors une seule racine ζ de l'unité satisfaisant la congruence $\zeta \equiv b_0 \pmod{\pi}$. Si on pose $v_1 = v_\mathfrak{p}(b_0^{N\mathfrak{p}-1} - 1)$, un calcul immédiat donne la minoration

$$v_\mathfrak{p}((b_0 + b_1\pi^{v_1})^{N\mathfrak{p}-1} - 1) \geqslant v_1$$

où b_1 est un élément du corps résiduel représenté comme ci-dessus. D'après le lemme de Hensel, il existe une seule valeur de b_1 pour laquelle on a

$$v_\mathfrak{p}((b_0 + b_1\pi^{v_1})^{N\mathfrak{p}-1} - 1) = v_2 > v_1.$$

En itérant ce procédé, on obtient une approximation aussi précise que l'on veut de la racine de l'unité attachée à la valeur b_0. Lorsque b_0 parcourt tous les éléments non nuls du corps résiduel (ou ± 1 lorsque $N\mathfrak{p} = 2$), on obtient toutes les racines de l'unité de $K_\mathfrak{p}$ et l'on peut déterminer l'exposant de p dans $\tilde{e}_\mathfrak{p}$.

Le calcul de la valuation logarithmique (qui fait intervenir les deux sections de ce paragraphe) est désormais possible.

5. STRUCTURE DU l-GROUPE DES CLASSES LOGARITHMIQUES

5.1. *Structure du l-groupe* $\widetilde{\mathcal{C}l}(l)$

LEMME 4. *Si* $g = 1$, *le groupe* $\widetilde{\mathcal{C}l}(l)$ *est trivial. Sinon, les classes logarithmiques des diviseurs* $\mathfrak{l}_i - \mathfrak{l}_1$ *pour* $i = 2, ..., g$ *forment un système de générateurs de* $\widetilde{\mathcal{C}l}(l)$.

Démonstration. Dans le cas où il n'y a qu'une seule place au-dessus du nombre premier l dans l'extension $K/\mathbb{Q}$, le résultat est évident.

Dans le cas contraire, considérons un diviseur logarithmique construit sur les g places sauvages $\mathfrak{l}_i$ et dont le degré sur K est nul. Comme K est galoisien sur $\mathbb{Q}$, la somme des coefficients de ce diviseur doit être nulle et les $g-1$ classes logarithmiques des diviseurs $\mathfrak{l}_i - \mathfrak{l}_1$ forment bien un système de générateurs.

Pour déterminer la structure de $\widetilde{\mathscr{C}l}(l)$ et un système de générateurs de ses sous-groupes cycliques, on peut procéder de la manière suivante: les combinaisons linéaires à coefficients entiers l-adiques entre les classes logarithmiques $[\mathfrak{l}_i - \mathfrak{l}_1]$ $(2 \leqslant i \leqslant g)$ s'écrivant: $\sum_{i=2}^{g} m_i[\mathfrak{l}_i - \mathfrak{l}_1] = 0$, $m_i \in \mathbb{Z}_l$. En termes de diviseurs logarithmiques, cela signifie qu'il existe un $\alpha \in \mathscr{K}$ tel que $\sum_{i=2}^{g} m_i(\mathfrak{l}_i - \mathfrak{l}_1) = \widetilde{d}(\alpha)$ où l'élément α appartient nécessairement au tensorisé par $\mathbb{Z}_l$ du groupe des l-unités de K (i.e. des unités globales en dehors des places sauvages). Ainsi, les relations entre les générateurs $[\mathfrak{l}_i - \mathfrak{l}_1]$ $(2 \leqslant i \leqslant g)$ sont toutes des combinaisons linéaires à coefficients dans $\mathbb{Z}_l$ des $r+g$ relations (où r est le degré de $K/\mathbb{Q}$ lorsque cette extension est réelle et la moitié de ce degré dans le cas contraire):

$$\sum_{i=2}^{g} \tilde{v}_{\mathfrak{l}_i}(\alpha_j)[\mathfrak{l}_i - \mathfrak{l}_1] = 0, \qquad j = 1, ..., r+g,$$

(α_j) décrivant un système (fini) de représentants de générateurs du groupe des l-unités.

A cause de son caractère élémentaire, nous ne donnons pas la description du calcul de la structure du l-groupe Cl'.

5.2. *Structure du conoyau de φ*

Dans ce sous-paragraphe et le suivant, on associe canoniquement à chaque idéal $\mathfrak{a} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m_\mathfrak{p}}$ le diviseur logarithmique: $\mathfrak{a}^* = \sum_{\mathfrak{p} \nmid l} (m_\mathfrak{p}/\lambda_\mathfrak{p})\, \mathfrak{p} + \sum_{j=1}^{g} m_{\mathfrak{l}_j} \mathfrak{l}_j$ et l'on note $\{\mathfrak{a}_i\}$ $(1 \leqslant i \leqslant h')$ les classes génératrices des h' composantes cycliques de $\mathscr{C}l'$.

Le morphisme η étant surjectif, le $\mathbb{Z}_l$-module principal $\deg_K \mathscr{D}$ est engendré par le degré d'un diviseur $\mathfrak{a}_i^*$ dont la l-valuation est minimale. Notons $\mathfrak{a}_{i_0}^*$ un tel diviseur. Le conoyau $\operatorname{Coker} \varphi \simeq \deg_K \mathscr{D}/(\deg_K \mathfrak{l})\, \mathbb{Z}_l$ est donc un l-groupe cyclique engendré par la classe du degré de $\mathfrak{a}_{i_0}^*$ d'ordre $l^{v_l(\deg_K \mathfrak{l}) - v_l(\deg_K \mathfrak{a}_{i_0}^*)}$.

5.3. *Structure du noyau de η*

Si l^n est l'ordre du conoyau de l'homomorphisme φ: $\widetilde{\mathscr{C}l} \to \mathscr{C}l'$, il est possible de construire la famille de diviseurs logarithmiques

$$\mathfrak{b}_{i_0} = l^n \mathfrak{a}_{i_0}$$

$$\mathfrak{b}_i = \mathfrak{a}_i \qquad \text{si} \quad 1 \leqslant i \leqslant h', \quad i \neq i_0 \quad \text{et} \quad \deg_K \mathfrak{a}_i^* \in (\deg_K \mathfrak{l})\, \mathbb{Z}_l$$

$$\mathfrak{b}_i = \mathfrak{a}_i - \frac{\deg_K \mathfrak{a}_i^*}{\deg_K \mathfrak{a}_{i_0}^*}\, \mathfrak{a}_{i_0} \qquad \text{sinon,}$$

puisque le nombre $\deg_K \mathfrak{a}_i^* / \deg_K \mathfrak{a}_{i_0}^*$ est, d'après le choix du diviseur $\mathfrak{a}_{i_0}^*$, un entier l-adique.

L'introduction de cette famille est motivée par le lemme suivant:

LEMME 5. *Les classes dans Cl' des diviseurs $\mathfrak{b}_i$ $(1 \leqslant i \leqslant h')$ engendrent le noyau H de l'homomorphisme η.*

Démonstration. Considérons un idéal $\mathfrak{a}$ dont la classe dans $\mathscr{C}l'$ appartient au noyau H. Par construction de classes $\{\mathfrak{a}_i\}$, il existe une famille d'entiers (m_i) $(1 \leqslant i \leqslant h')$ telle que: $\{\mathfrak{a}\} = \prod_{i=1}^{h'} \{\mathfrak{a}_i\}^{m_i}$ dans $\mathscr{C}l'$; ce qui en termes de diviseurs logarithmiques, s'écrit, modulo les places sauvages du corps, sous la forme: $\mathfrak{a} \equiv \sum_{i=1}^{h'} m_i \mathfrak{a}_i$ ou encore $\mathfrak{a}^* \equiv \sum_{i=1}^{h'} m_i \mathfrak{a}_i^*$. Notons I l'ensemble des indices $i \neq i_0$ tels que la classe de $\mathfrak{a}_i^*$ appartiennent à H et J celui des indices $i \neq i_0$ n'appartenant pas à I puis μ_i $(i \in I)$ l'entier l-adique $\deg_K \mathfrak{a}_i^* / \deg_K \mathfrak{a}_{i_0}^*$. Modulo les degrés des places sauvages, nous avons les congruences:

$$\begin{aligned} \deg_K \mathfrak{a}^* &\equiv \sum_{i=1}^{h'} m_i \deg_K \mathfrak{a}_i^* \\ &\equiv \sum_{i \in I} m_i \deg_K \mathfrak{b}_i^* + \sum_{i \in J} m_i \deg_K \mathfrak{b}_i^* \\ &\quad + \left(m_{i_0} + \sum_{i \in J} m_i \mu_i \right) \deg_K \mathfrak{a}_{i_0}^*. \end{aligned}$$

La première somme du second membre est congrue à 0 par définition de I, la deuxième somme est nulle d'après la définition des $\mathfrak{b}_i$ $(i \in J)$, et l'on obtient finalement:

$$\deg_K \mathfrak{a}^* \equiv \left(m_{i_0} + \sum_{i \in J} m_i \mu_i \right) \deg_K \mathfrak{a}_{i_0}^*.$$

Comme $\deg_K \mathfrak{a}_{i_0}^*$ est un générateur du $\mathbb{Z}_l$-module $\deg_K \mathscr{D}$, l'entier l-adique $m_{i_0} + \sum_{i \in J} m_i \mu_i$ est un multiple de l'ordre l^n du conoyau de φ et il existe un entier l-adique u tel que: $m_{i_0} + \sum_{i \in J} m_i \mu_i = l^n u$. Le diviseur $\mathfrak{a}$ satisfait donc les congruences:

$$\mathfrak{a} \equiv \sum_{\substack{i=1 \\ i \neq i_0}}^{h'} m_i \mathfrak{a}_i + \left(l^n u - \sum_{i \in J} m_i \mu_i \right) \mathfrak{a}_{i_0} \equiv \sum_{\substack{i=1 \\ i \neq i_0}}^{h'} m_i \mathfrak{b}_i + u \mathfrak{b}_{i_0}:$$

ce qui achève la démonstration.

Pour déterminer la structure du groupe H et un système de générateurs $\{\mathfrak{b}_i'\}$ de manière à ce que: $H = (\mathbb{Z}/b_1\mathbb{Z})\{\mathfrak{b}_1'\} \oplus \cdots \oplus (\mathbb{Z}/b_k\mathbb{Z})\{\mathfrak{b}_k'\}$, on utilise la méthode décrite dans [C-D-O] pour le calcul du noyau dans une suite exacte.

5.4. *Structure de* $\widetilde{\mathscr{C}l}$

Pour chacun des diviseurs $\mathfrak{b}'_i$ $(1 \leqslant i \leqslant k)$, on considère la famille d'entiers l-adiques $(m_{\mathfrak{p}}^{(i)})_{\mathfrak{p} \in P}$ telle que $\mathfrak{b}'_i = \sum_{\mathfrak{p} \in P} m_{\mathfrak{p}}^{(i)} \mathfrak{p}$ et l'on construit le relèvement dans $\widetilde{\mathscr{C}l}$,

$$\mathfrak{b}''_i = \sum_{\mathfrak{p} \in P} \frac{m_{\mathfrak{p}}^{(i)}}{\lambda_{\mathfrak{p}}} \mathfrak{p} + \mu_i \mathfrak{l}_1 \qquad \text{où} \qquad \mu_i = -\sum_{\mathfrak{p} \in P} \frac{m_{\mathfrak{p}}^{(i)}}{\lambda_{\mathfrak{p}}} \cdot \frac{\deg_K \mathfrak{p}}{\deg_K \mathfrak{l}_1} \in \mathbb{Z}_l$$

de sorte que $\mathfrak{b}''_i$ soit effectivement de degré nul sur K.

Par définition des ordres b_i des différentes composantes cycliques de H, il existe une famille d'entiers $(v_i)_{1 \leqslant i \leqslant k}$ premiers à l, des éléments $(\alpha_i)_{1 \leqslant i \leqslant k}$ de $\mathscr{K}$ et une suite $(n_{ij})_{1 \leqslant i \leqslant k}$ d'entiers l-adiques tels que:

$$v_i b_i \mathfrak{b}'_i = \sum_{\mathfrak{p} \in P} v_{\mathfrak{p}}(\alpha_i)\, \mathfrak{p} + \sum_{j=1}^{g} n_{ij} \mathfrak{l}_j, \qquad 1 \leqslant i \leqslant k.$$

Pour déterminer les éléments α_i pour $1 \leqslant i \leqslant k$, on forme la matrice A dont les colonnes correspondent à la décomposition des idéaux premiers au-dessus de l dans le groupe des classes au sens ordinaire. On concatène cette matrice avec le vecteur colonne Y_i donnant la décomposition de l'idéal $v_i b_i \mathfrak{b}'_i$ puis avec la matrice B, sous forme normale de Smith, qui donne la structure du groupe des classes. On appelle U la matrice unimodulaire qui permet de réduire $(A \mid Y_i \mid B)$ à sa forme normale d'Hermite. Soit $U_1 = (u_{ij})$ la sous-matrice de U formée des $g+1$ premières lignes et colonnes. Comme chaque idéal $v_i b_i \mathfrak{b}'_i$ est principal dans $\mathscr{C}l'$, la $(g+1)$-ième ligne de la matrice U_1 contient, à une colonne k-ième, une composante u_{g+1k} qui est inversible modulo le nombre de classes, de sorte que l'idéal $(v_i b_i \mathfrak{b}'_i) \cdot (\prod_{j=1}^{g} \mathfrak{l}_j^{u_{jk}})^b$, où b est un relèvement de l'inverse de u_{g+1k} modulo le nombre de classes, soit principal dans le groupe des classes. Un générateur de cet idéal principal donne l'élément α_i cherché.

À présent, notons $(\delta_q)_{1 \leqslant q \leqslant t}$ les générateurs des t composantes cycliques du l-groupe $\widetilde{\mathscr{C}l}(l)$: $\widetilde{\mathscr{C}l}(l) = (\mathbb{Z}/r_1\mathbb{Z})\,\delta_1 \oplus \cdots \oplus (\mathbb{Z}/r_t\mathbb{Z})\,\delta_t$. La matrice de relations entre les générateurs $v_1 \mathfrak{b}''_1, ..., v_k \mathfrak{b}''_k, \delta_1, ..., \delta_t$ de $\widetilde{\mathscr{C}l}$ est (cf. [C-D-O]) une matrice de la forme: $F = \begin{pmatrix} B & 0 \\ -P & R \end{pmatrix}$ où B est la matrice décrite ci-dessus, R la matrice de Smith de $\widetilde{\mathscr{C}l}$ et P la matrice exprimant les classes logarithmiques des diviseurs $v_i b_i \mathfrak{b}''_i$ $(1 \leqslant i \leqslant k)$ en fonction des classes génératrices δ_q $(1 \leqslant q \leqslant t)$ du l-groupe $\widetilde{\mathscr{C}l}(l)$. Pour déterminer la matrice P, nous cherchons dans une première étape, à exprimer chacune des classes

$\{v_i b_i \mathfrak{b}_i''\}$ en fonction des classes génératrices $[\mathfrak{l}_j - \mathfrak{l}_1]$ $(1 \leqslant j \leqslant g)$. Comme pour tout i $(1 \leqslant i \leqslant k)$ et tout j $(1 \leqslant j \leqslant g)$ on a

$$v_i b_i m_{\mathfrak{p}}^{(i)} = v_{\mathfrak{p}}(\alpha_i), \qquad \forall \mathfrak{p} \nmid l$$
$$v_i b_i m_{\mathfrak{l}_j}^{(i)} = v_{\mathfrak{l}_j}(\alpha_i) + n_{ij},$$

les diviseurs $v_i b_i \mathfrak{b}_i''$ $(1 \leqslant i \leqslant k)$ s'écrivent:

$$v_i b_i \mathfrak{b}_i'' = \sum_{\mathfrak{p} \nmid l} \frac{v_i b_i m_{\mathfrak{p}}^{(i)}}{\lambda_{\mathfrak{p}}} \mathfrak{p} + \mu_i v_i b_i \mathfrak{l}_1 = \sum_{\mathfrak{p} \nmid l} \tilde{v}_{\mathfrak{p}}(\alpha_i)\, \mathfrak{p} + \mu_i v_i b_i \mathfrak{l}_1$$

$$v_i b_i \mathfrak{b}_i'' = \sum_{\mathfrak{p} \in P} \tilde{v}_{\mathfrak{p}}(\alpha_i)\, \mathfrak{p} + (\mu_i v_i b_i - \tilde{v}_{\mathfrak{l}_1}(\alpha_i))\, \mathfrak{l}_1 - \sum_{j=2}^{g} \tilde{v}_{\mathfrak{l}_j}(\alpha_i)\, \mathfrak{l}_j.$$

Comme $v_i b_i \mathfrak{b}_i''$ est un diviseur de degré nul, on a nécessairement

$$\sum_{j=1}^{g} \tilde{v}_{\mathfrak{l}_j}(\alpha_i) = \mu_i v_i b_i$$

et on obtient finalement: $v_i b_i \mathfrak{b}_i'' = \widetilde{d}(\alpha_i) - \sum_{j=2}^{g} \tilde{v}_{\mathfrak{l}_j}(\alpha_i)(\mathfrak{l}_j - \mathfrak{l}_1)$. Modulo les diviseurs logarithmiquement principaux, l'expression des diviseurs $v_i b_i \mathfrak{b}_i''$ en fonction des diviseurs $\mathfrak{l}_j - \mathfrak{l}_1$ est: $[v_i b_i \mathfrak{b}_i''] = -\sum_{j=2}^{g} \tilde{v}_{\mathfrak{l}_j}(\alpha_i)[\mathfrak{l}_j - \mathfrak{l}_1]$. La matrice P est donc le produit RQ où Q est la matrice dont les coefficients sont $q_{ji} = \tilde{v}_{\mathfrak{l}_j}(\alpha_i)$, $(2 \leqslant j \leqslant g,\ 1 \leqslant i \leqslant r+g)$ et R la matrice à t colonnes et $g-1$ lignes exprimant chacune des classes logarithmiques $[\mathfrak{l}_j - \mathfrak{l}_1]$ en fonction des générateurs δ_q de $\widetilde{\mathscr{C}l}(l)$. Cette dernière est l'inverse de la matrice, déjà utilisée, pour déduire les générateurs δ_q à partir des générateurs $[\mathfrak{l}_j - \mathfrak{l}_1]$.

Les réductions successives d'Hermite et de Smith de la matrice F donnent la structure complète du l-groupe des classes logarithmiques.

6. EXEMPLES NUMERIQUES

Le groupe des classes logarithmiques a été numériquement étudié seulement dans des cas très particuliers: quand $l = 2$, on a un critère de cyclicité du groupe des classes logarithmiques dans le cadre des extensions de type CM (cf. [S_2]), de trivialité dans le cadre des corps quadratiques (cf. [S_1]) et l'on connaît la structure du groupe des classes logarithmiques de corps biquadratiques contenant les racines quatrièmes de l'unité et dont la 2-partie du noyau hilbertien est triviale (cf. [T]). Pour $l = 3$, un calcul explicite du groupe des classes logarithmiques de certains corps quadratiques est donné dans [Z].

Nous avons mis en pratique les algorithmes décrits dans cet travail et nous avons construit le groupe des classes logarithmiques pour tous les corps biquadratiques $K = \mathbb{Q}(i, \sqrt{d})$ dans le cas $l = 2$ et tous les corps biquadratiques $K = \mathbb{Q}(\sqrt{-3}, \sqrt{d})$ dans le cas $l = 3$ lorsque d est le discriminant d'un corps quadratique réel et $4 < d \leqslant 2000$. Comme ces corps contiennent, respectivement, les racines quartiques et sextiques de l'unité, on sait que le l-rang du groupe des classes logarithmiques de ces corps et le l-rang de la l-partie du noyau hilbertien sont égaux. Nous pouvons ainsi allonger la liste des corps de nombres dont on sait calculer le l-rang du noyau hilbertien (cf. par exemple, [BG], [BS] et [CK]):

PROPOSITION 6. *Le corps biquadratique contenant les racines cubiques de l'unité de plus petit discriminant pour lequel le* 3*-groupe des classes logarithmiques est non trivial est le corps* $K = \mathbb{Q}(\sqrt{-3}, \sqrt{29})$ *de discriminant* 7569. *Ce corps est engendré par une racine du polynôme* $P(X) = X^4 - 2X^3 - 55X^2 + 56X + 871$.

Démonstration. Il est facile de vérifier que l'on a $\mathcal{C}l \simeq \mathbb{Z}/3\mathbb{Z}$ et que ce groupe est engendré par la classe représentée par l'idéal premier au-dessus de 2: $\mathfrak{p}_2 = 2\mathbb{Z}_K + \alpha\mathbb{Z}_K$ avec $\alpha = \frac{1}{2}(\theta^2 + 3\theta + 1)$, où $P(\theta) = 0$.

Il n'y a qu'une place sauvage $\mathfrak{p}_3 = 3\mathbb{Z}_K + (\theta^2 - \theta - 1)\,\mathbb{Z}_K = 1/119(2\theta^3 - 3\theta^2 - 52\theta - 152)\,\mathbb{Z}_K$ pour laquelle on a $e_{\mathfrak{p}_3} = f_{\mathfrak{p}_3} = 2$. Ceci montre que le 3-groupe $\mathcal{C}l(3)$ est trivial et on a $\mathcal{C}l' \simeq \mathcal{C}l$. La partie sans torsion du 3-groupe des unités est engendrée par le générateur de $\mathfrak{p}_3$ et par l'unité $\varepsilon = 1/238(9\theta^3 + 46\theta^2 - 234\theta - 1279)$.

D'autre part, les valuations en 3 des degrés des diviseurs $\mathfrak{p}_3$ et $\mathfrak{p}_2^{\lambda_{\mathfrak{p}2}}$ sont égales et le conoyau de φ est trivial. On en déduit que l'on a $H = \mathcal{C}l'$ (cf. Section 3); ceci conduit à l'isomorphisme cherché $\widetilde{\mathcal{C}l} \simeq \mathcal{C}l' \simeq \mathbb{Z}/3\mathbb{Z}$ puisque le fait d'avoir une seule place sauvage prouve que $\widetilde{\mathcal{C}l}(l)$ est aussi trivial (cf. Lemme 4).

Finalement, le générateur de $\widetilde{\mathcal{C}l}$ est la classe représentée par le diviseur $(2 + 3 + 3^2 + 3^3 + 3^4 + 3^5 + 3^6 + O(3^7))\,\mathfrak{p}_2 + (1 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 3^4 + 2 \cdot 3^5 + 2 \cdot 3^6 + O(3^7))\,\mathfrak{p}_3$ dont il est facile de vérifier que son degré est 0.

Par la suite, nous donnons un exemple de corps K pour chacun des groupes de classes logarithmiques que nous avons obtenu. Nous rappelons que le corps K est de la forme $K = \mathbb{Q}(i, \sqrt{d})$ lorsque $l = 2$ et de la forme $K = \mathbb{Q}(\sqrt{-3}, \sqrt{d})$ lorsque $l = 3$. Pour chaque corps cité, nous indiquons la valeur de d, le nombre de classes logarithmiques noté $\tilde{h}$ et la structure de ce groupe sous la forme $[a_1, ..., a_s]$.

Cas $l=2$

d	$\tilde{h}$	$\widetilde{\mathcal{C}l}$	d	$\tilde{h}$	$\widetilde{\mathcal{C}l}$	d	$\tilde{h}$	$\widetilde{\mathcal{C}l}$
17	2	[2]	85	4	[2, 2]	161	32	[8, 4]
41	4	[4]	113	8	[4, 2]	185	8	[8]
221	16	[8, 2]	1020	64	[32, 2]	1221	64	[8, 8]
357	8	[2, 2, 2]	1085	32	[16, 2]	1241	32	[8, 2, 2]
445	16	[4, 4]	1105	16	[4, 2, 2]	1365	32	[4, 2, 2, 2]
521	16	[16]	1173	16	[2, 2, 2, 2]	1769	32	[32]
561	32	[4, 4, 2]	1217	128	[16, 8]	1820	1024	[512, 2]

Cas $l=3$

d	$\tilde{h}$	$\widetilde{\mathcal{C}l}$	d	$\tilde{h}$	$\widetilde{\mathcal{C}l}$	d	$\tilde{h}$	$\widetilde{\mathcal{C}l}$
141	9	[9]	321	27	[9, 3]	1373	81	[27, 3]
253	9	[3, 3]	969	27	[27]	1901	81	[9, 3, 3]

BIBLIOGRAPHIE

[BG] J. Browkin et H. Gangl, Table of tame and wild kernels of quadratic imaginary number fields of discriminants > -5000 (conjectural values), Institut für Experimentelle Mathematik, Vol. 20, preprint.

[BS] J. Browkin et A. Schinzel, On Sylow 2-subgroups of $K_2(\mathcal{O}_F)$ for quadratic number fields F, *J. Reine Angew. Math.* **331** (1982), 104–113.

[C] H. Cohen, "A Course in Computational Algebraic Number Theory," Graduate Text in Mathematics, Vol. 138, Springer-Verlag, Berlin/Heidelberg/New York, 1993.

[C-D-O] H. Cohen, F. Diaz y Diaz, et M. Olivier, Algorithmic methods for finitely generated abelian groups, *Symbolic Comput*. (1997), to appear.

[CK] A. Candiotti et K. Kramer, On the 2-Sylow subgroup of the Hilbert kernel of K_2 of number fields, *Acta Arith.* **L II** (1989), 49–65.

[D-O] F. Diaz y Diaz et M. Olivier, Algorithmique Algébrique dans les Corps de Nombres, État de la Recherche en Algorithmique Arithmétique, Laboratoire A2X Bordeaux, 1995.

[H-M] J. Hafner et K. McKurley, A rigorous sous exponential algorithm for computation of class groups, *J. Ann. Math. Soc.* **2** (1989), 837–850.

[J_1] J.-F. Jaulent, Noyau universel et valeurs absolues, Journées Arithmétiques de Marseille-Luminy, *Astérisque* **198-199-200** (1991), 187–207.

[J_2] J.-F. Jaulent, Sur le noyau sauvage des corps de nombres, *Acta Arith.* **67** (1994), 335–348.

[J_3] J.-F. Jaulent, Classes logarithmiques des corps de nombres, *J. Théor. Nombres Bordeaux* **6** (1994), 307–327.

[J_4] J.-F. Jaulent, Classes logarithmiques des corps de nombres totalement réels, Pré-publication.

[P] D. Bernardi, C. Batut, H. Cohen, et M. Olivier, “User's Guide to PARI-GP, Version 1.39,” Publ. Université Bordeaux I, 1991.

[S_1] F. Soriano, Classes logarithmiques ambiges des corps quadratiques, *Acta Arith.* **78** (1997), 201–219.

[S_2] F. Soriano, Sur les classes logarithmiques des (CM)-extensions, *C. R. Acad. Sci. Paris Sér. I Math.* **324** (1997), 737–739.

[T] H. Thomas, Trivialité du 2-rang du noyau hilbertien, *J. Théor. Nombres Bordeaux* **6** (1994), 459–483.

[Z] T. S. Zran Zankoe, “Noyau des valeurs absolues 3-adiques,” Thèse de l'Université Bordeaux, (1991).